

DESIGN AND DEVELOPMENT OF A MICROCONTROLLER BASED WIRELESS SECURITY ACCESS SYSTEM

¹Adewale A. A., ²Abdulkareem A., ³Agbetuyi A. F., ⁴Dike Ike

Department of Electrical and Information Engineering, Covenant University, Ota, Nigeria

Abstract- Security can simply be protecting your equipment and files from unauthorized access, but there is much more. Computer security helps ensure that your computers, networks, and peripherals work as expected all the time, and that your data is safe in the event of hard disk crash or a power failure resulting from an electrical storm. Security makes sure no damage is done to your data and that no one is able to read it unless you want them to. This work focuses on security from the dimension of remote wireless access using password credential. In various industries, companies and even homes of today, the use of this means of security is very popular and various evolution over the years have been made to the first model that came out in the late 1800's. The main activities involved in this work are the research done on how the automatic gate works and the transfer of frequency modulated signals using the transmitter and receiver module.

Keywords- Password, Remote Wireless Access, Receiver, Security, Transmitter

I. INTRODUCTION

Access control is the ability to permit or deny the use of a particular resource by a particular entity [1]. In order to protect their systems from attacks, organizations have evolved various procedures and systems aimed at protecting information assets from both internal and external threats. An access control point, which can be a door, turnstile, parking gate, elevator, or other physical barrier where granting access can be electrically controlled [2].

Typically the access point is a door having several elements, at its most basic there is a stand-alone electronic lock [3]. In larger applications involving more than one door electric strikes or magnetic locks are used. The lock is unlocked by an operator with a switch. To automate this, operator intervention is replaced by a reader. The reader could be a keypad where a code is entered, it could be a card reader, or it could be a biometric reader. Readers do not usually make an access decision but send a card number to an access control panel that verifies the number against an access list. Generally only entry is controlled and exit is uncontrolled. In cases where exit is also controlled a second reader is used on the opposite side of the door. In cases where exit is not controlled, free exit, a device called a request-to-exit (REX) is used. Request-to-exit devices can be a pushbutton or a motion detector. When the button is pushed or the motion detector detects motion at the door, the door alarm is temporarily ignored while the door is opened. Exiting a door without having to electrically unlock the door is called mechanical free egress. This is an important safety feature. In cases where the lock must be electrically unlocked on exit, the request-to-exit device also unlocks the door.

This system deals with access control as regard to the entry of an individual or a vehicle into a given vicinity. An individual possessing the password that is programmed to the device is able to have access only to the area that is being safeguarded by the security system, thereby prohibiting entry of another individual without due authorization. This device can be used in a number of areas such as offices, hotels, banks, organizations and even homes. This is depending on what the individual intend to safe guard. With this project, the scenario painted is the safe guarding of a homeowners gate whereby the owner chooses to enter his home, then keys the pass code which then gives him/her entrance into the vicinity.

II. OVERVIEW OF THE SYSTEM

This system uses a PIC 16F84 microcontroller for the transmitter design and PIC16F84 for the receiver module. The operation of the system is simple. The PIN for the person to be granted access is stored in selected general purpose registers in the controller. The microcontroller scans the data entry, and compares it with the stored PIN to grant or deny access to the person [3]. The generalized block diagram for the design is found in Fig 1.1.

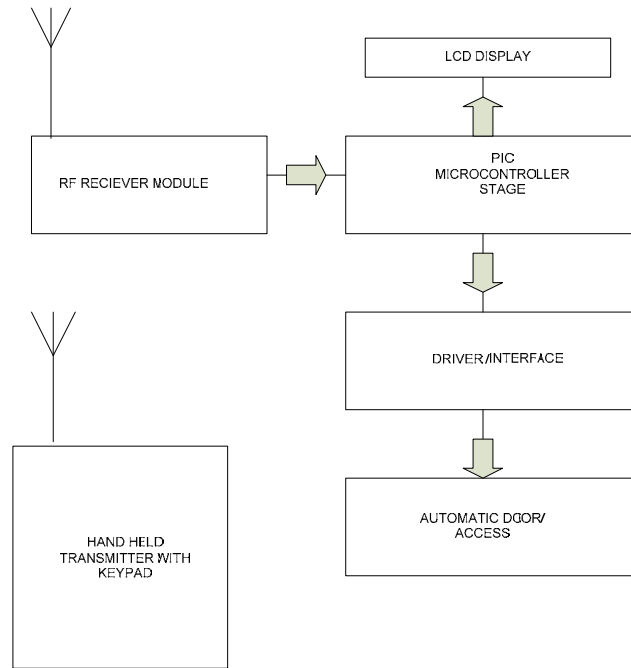


FIG 1.1 GENERALIZED BLOCK DIAGRAM : REMOTE ACCESS CONTROL SYSTEM

III. SYSTEM ARCHITECTURE

This section is based on the detailed plan and outline on how the system is designed as the chapter is aptly named. In subsequent headings; we shall be looking at the equipments used in ultimately realizing the finished product. The interfaces, equipments and also the component used in each stage of this prototype assembly and construction.

Input Type: Telephone Keypad, Pin: 3 Digits; Password: 464; Transmitter Frequency: 415MHZ; Supply Voltage: 5vdc, 12vdc (For Model Gate Dc Motors) Maximum Current: 500ma Access Mechanism: Model Sliding Door Microcontroller: PIC16F84 Sliding Door Interconnect: Small Computer System Interconnect (SCSI); DB-9 connector. The starting point of the project begins with the remote control (transmitter). On this remote, is placed a keypad possessing a 12Key 3x4 matrix keypad connected to the PORTB of the microcontroller, which has been configured as the input. The microcontroller scans the PORTB using a special subroutine program (SCAN), and decodes any of the depressed keypads then sends the decoded binary number to register where it is compared with the stored numbers. If all the entered numbers give the saved numbers programmed in the special register, the microcontroller then sends a signal to modulate the transmitter. The signal modulates a 415MHz transmitter module capable of about 50meters. Supposing the numbers which are keyed on the keypad are not programmed in the special register or not keyed in the particular order as that saved in the special register, the access denied LED is set off which has been configured on PORTA3. When the correct code has been keyed in the correct order; the access granted LED is set off which is configured on PORTA2 and in turn; an electric pulse is sent to the Relay (RL1) via PORTA1. PORTA has been configured as an output port. After the relay has been sent to the RELAY (RL1), the magnetic field created by the armature coil attracts the armature to connect the contact thereby connecting the circuit and the signal being sent to the receiver.

On the receiver end, the signal is demodulated by the receiver module which sends the pulse to the PORTA1 of the microcontroller which has been configured as the input, and the output is now sent to the relays (RL1 AND RL2) via the transistors Q1 and Q2 that controls the opening and closing of the model door via PORTB6 and PORTB7. The system is also coded such that the output of PORTA2 on the transmitter module indicates ACCESS DENIED when the wrong code is sent, while the LCD indicates ACCESS GRANTED via PORTB0 to PORTB5.

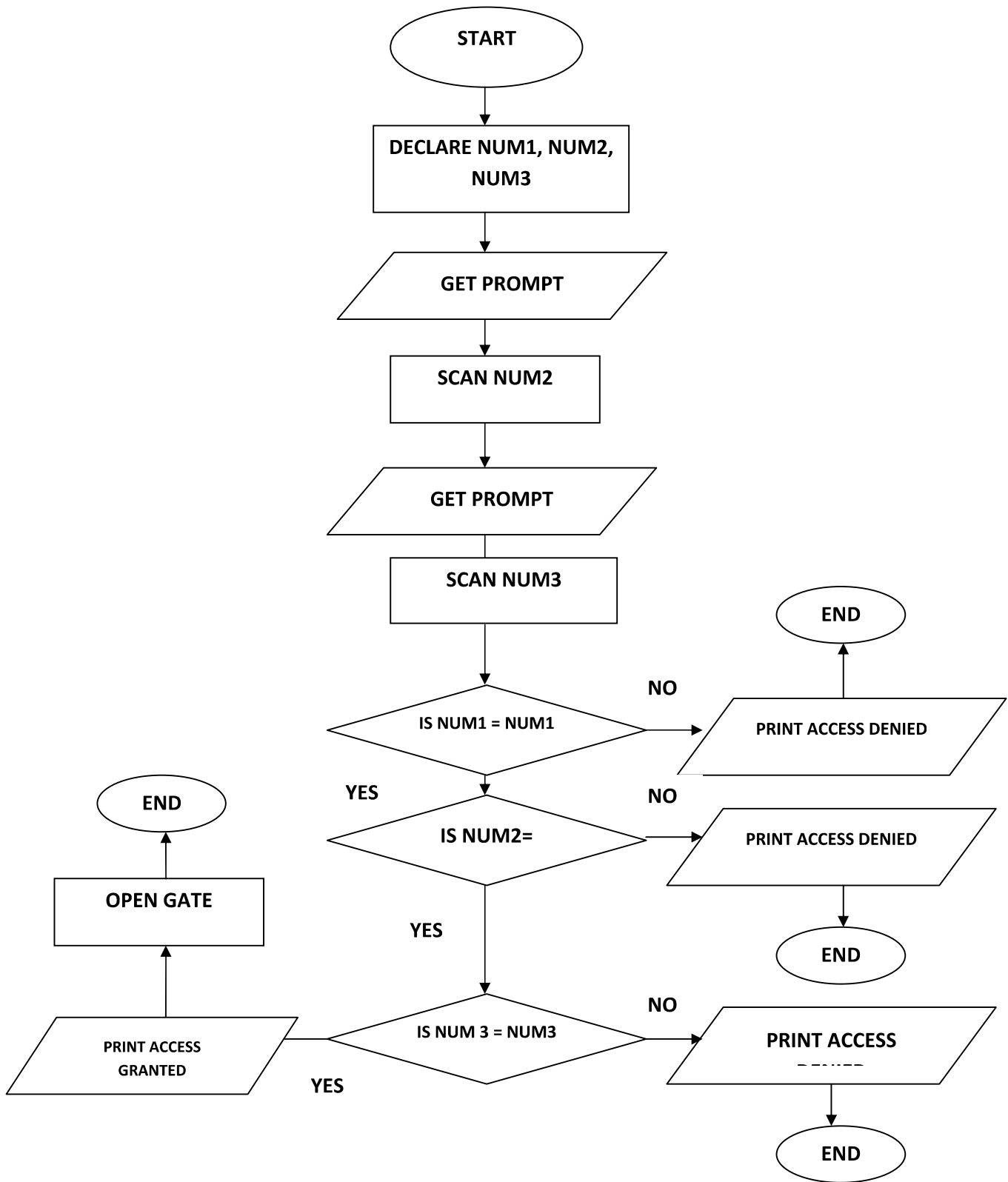


Figure 2. A FLOW DIAGRAM SHOWING THE PROCESS ALGORITHM

As earlier stated, the remote control possesses a 12 key keypad of 3x4 matrix format that require 7 connections to be made to the microcontroller (Dave Smith, 2006). Consider the 12 key keypad, there are seven connections to the keypad; C1, C2, C3, R1, R2, R3, R4. This is arranged in 3 columns and 4 rows as shown in Table 1.

TABLE 1. A 12 KEY KEYPAD

	Column1,C1	Column2,C2	Column3,C3
Row1,R1	1	2	3
Row2,R2	4	5	6
Row3,R3	7	8	9
Row4,R4	*	0	#

The keypad works in the following way:

If for example key 6 is pressed then PORTB2 will be joined to PORTB4. For key 1, PORTB0 would be joined to B3 etc. as shown in Fig.3. In the case of key 1 being the number that is pressed; the microprocessor would set B0 low and scan B3, B4, B5 and B6 for a low to see if keys 1, 4, 7 or * had been pressed. In the case of key 5 being the number that is pressed The microcontroller would then set B1 low and scan B3, B4, B5 and B6 for a low to see if keys 2, 5, 8 or 0 had been pressed. In the case of key 9 being the number that is pressed Finally B2 would be set low and B3, B4, B5 and B6 scanned for a low to see if keys 3, 6, 9 or # had been pressed.

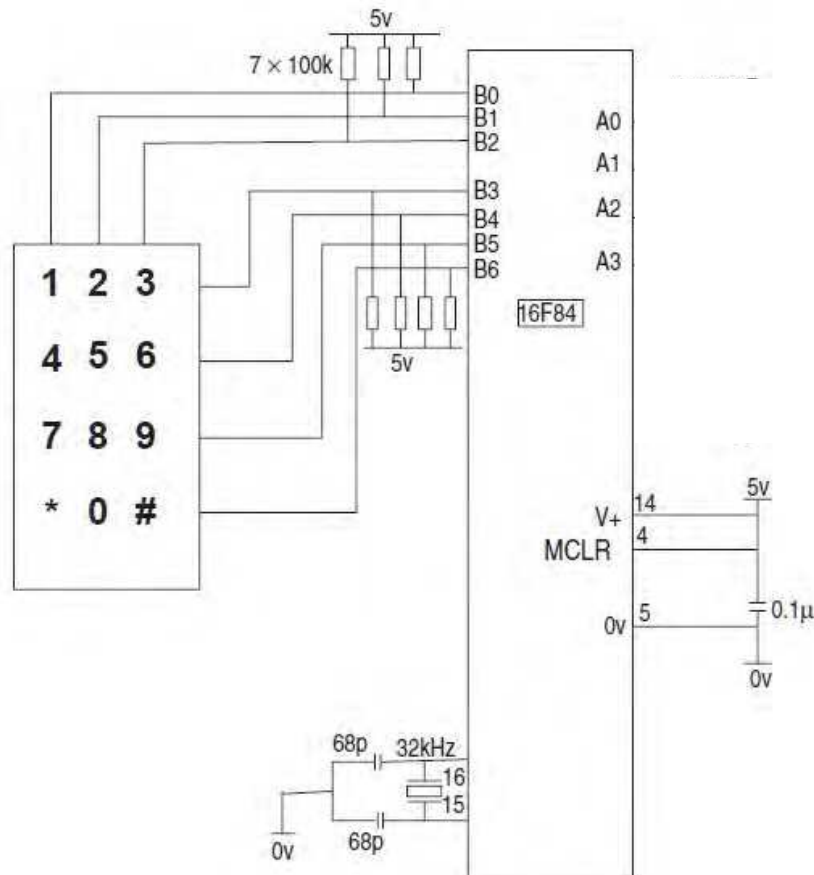


Figure 3. Diagram of keypad connection to the PIC 16F84

IV. SYSTEM DESIGN AND IMPLEMENTATION

The remote control transmitter module operating at 415 MHz frequency using simplex transmission for the purpose of ending the code to the receiver while the receiver “listens” for the code. The transmitter module is the only feasible approach. This is because at this frequency the design has to be on PCB because of problems of miller effect and other capacitance effect that occurs at very high frequencies. However part of the transmitter stage would be analyzed. The amplifier stage of the transmitter circuit is similar to that shown in Fig.4.

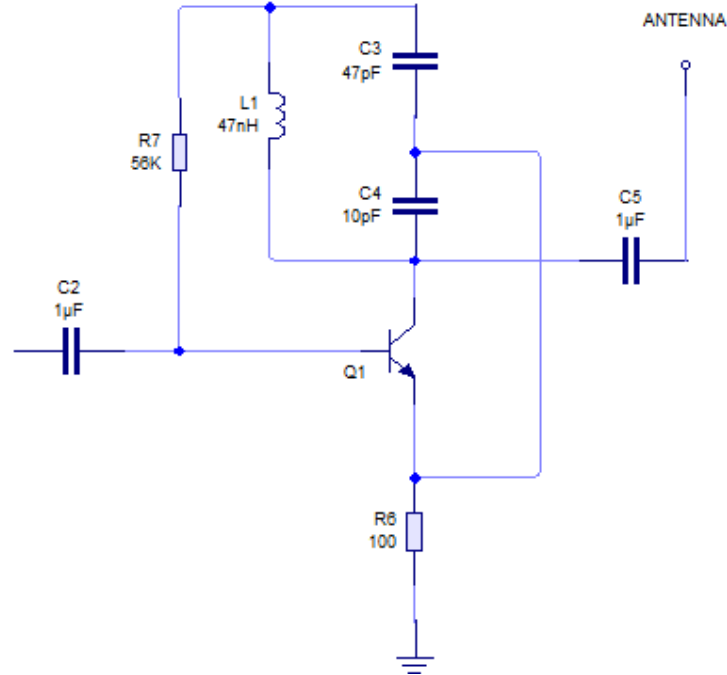


Figure 4. Transmitter circuit Amplifier stage.

The transmitter is a tuned RF class A amplifier. R7 gives the dc operating point bias, while the total reactance of the collector gives the collector bias. For class A bias,

$$V^+ = I_B R_B + V_{CE} + V_E \text{ ----- (2b)}$$

for best operating point in the active region, $V_{CE} + V_E = 0.5V_{CC} = 6V$.

for a power of 100mW,

$$I_C = \frac{P_{diss}}{V^+} = \frac{100mW}{12V} = 8.3mA$$

$$\text{but } H_{FE} = \frac{I_C}{I_B}$$

hence, $I_B = 27.6\mu A$ (where $H_{FE} = 300$, from data sheets for BC337 transistor).

from (2b), $R_B = 217.39K = 220K$ (preferred value).

$$V^+ = I_B R_B + V_{CE} + V_E \text{-----} (2b)$$

for best operating point in the active region, $V_{CE} + V_E = 0.5V_{CC} = 6V$.

for a power of 100mW,

$$I_C = \frac{P_{diss}}{V^+} = \frac{100mW}{12V} = 8.3mA$$

$$\text{but } H_{FE} = \frac{I_C}{I_B}$$

hence, $I_B = 27.6\mu A$ (where $H_{FE} = 300$, from data sheets for BC337 transistor).

from (2b), $R_B = 217.39K = 220K$ (preferred value).

Hence $R_7 = 220K\Omega$.

The frequency of the colpitts oscillator is given by,

$$f_{osc} = \frac{1}{2\pi\sqrt{L\left(\frac{C_1C_2}{C_1+C_2}\right)}}$$

The PIC 16F84 microcontroller is the main processing unit for this project. Its job is to perform timing and control functions accurately, as well as decode the signal sent from the transmitter module which opens and closes the automatic door access. The choice of PIC is not really critical since the project required just basic control and timing operations. The PIC 16F84 has 1K of program memory, 13I/O and 1 8bit extra timer. This was sufficient for our processor need which required less than 1K of program memory and 4 I/O. PORTA is configured as input, while PORTB as output. The circuit for the microcontroller stage is shown in Fig. 5.

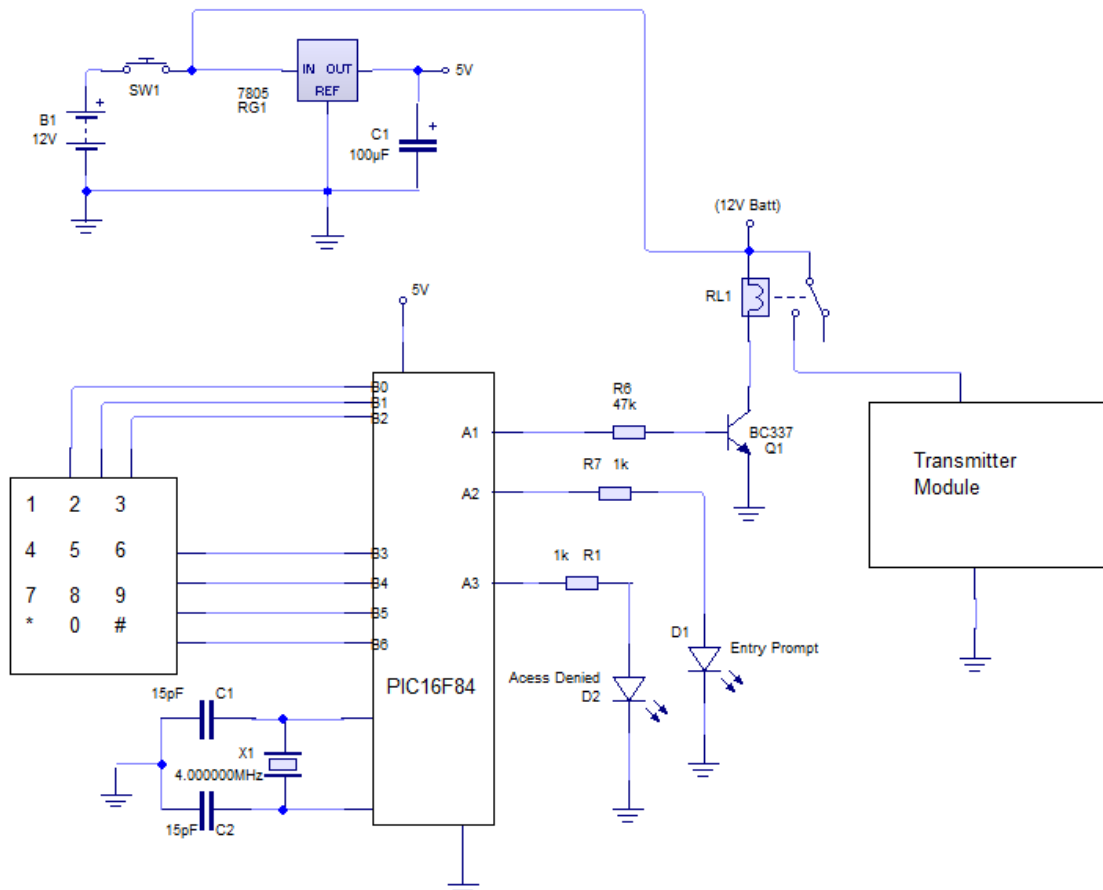


FIG 3.5a Transmitter stage circuit Diagram: Wireless Access Control System

Figure 5. Transmitter Stage

The model gate is controlled by transistor switching stages which control the DC motor that opens and close the gate. The signals that open and close the gate are generated from the PIC PORTB6 and PORTB7. These signals go to the transistor stage which sends electrical signal to the RL1 which control the sliding open of the door, then after 10 seconds, sends electrical signals to the second relay witch then controls the closing of the sliding door via the DC motor.

The switching transistor switches the relay, which controls the DC motors. The relay is switched on when PORTB6 and B7 are set to 1 complementarily. The controller makes sure B6 and B7 are mutually exclusive to ensure the door is opened and closed properly. A base resistor is required to ensure perfect switching of the transistor to saturation. Diode D1 & D2 protects the transistor from back EMF that might be generated since the relay coil presents an inductive load.

In this case R_C , which is the collector resistance, is the resistance of the relay coil, which is 400Ω for the relay type used in this work.

To find the value of the resistor in series with the base of the transistor

$R_C = 400\Omega$ (Relay coil resistance)

$V_+ = 12V$ (relay voltage from 12V regulator)

$V_{be} = 0.6V$ (silicon)

$V_{ce} = 0V$ (when transistor is switched)

$V_{in} = 5V$ (from microcontroller RB6, RB7)

$H_{fe} = 300$ (from transistor data sheets for BC337)

since for class A Amplifier,

$$V_+ = I_C R_C + V_{ce} \text{-----(4)}$$

$$V_{in} = I_b R_b + V_{be} \text{-----(5)}$$

$$H_{fe} = \frac{I_C}{I_b} \text{-----(6)}$$

from (5),

$$R_b = \frac{V_{in} - V_{be}}{I_b} \text{-----(7)}$$

Where,

I_C = collector current

I_B = base current

V_{in} = input voltage

V_t = supply voltage

V_{CE} = collector-emitter voltage

H_{fe} = current gain.

from (4) ,

$$I_c = \frac{12 - 0}{400} \\ = 0.03A.$$

from (6),

$$I_b = \frac{0.03}{300} \\ = 100\mu A$$

now using equation (7)

$$R_b = \frac{5 - 0.6}{100 \times 10^{-6}} \\ = 44K\Omega \\ = 47K\Omega \text{ (preferred value)}$$

$R_B = R_1 = R_2 = 47K$ (unit 3.3).

The power supply stage provides the appropriate DC voltage requirements to ensure the circuit components (especially the PIC) are powered properly. The PIC requires a maximum voltage of +6V, which makes a 5V power supply OK for the circuit. The 12V supply rail powers the relays which due to specifications require 12V. The power supply stage is a linear power supply type and involves in step down transformer, Rectifier, Filter capacitor, and voltage regulators, to give the various voltage levels.

The circuit for the power supply stage is shown in Fig 6.

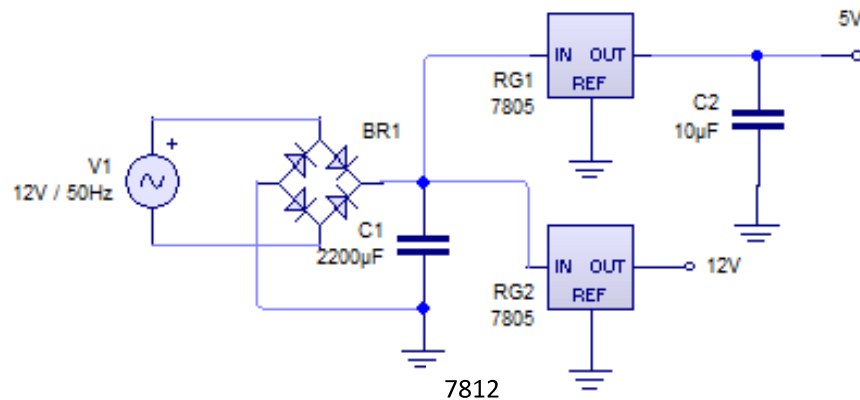


Figure 6. Power Supply Stage.

Regulator (7805 and 7812) is used to stabilize the voltage after it has been filtered. In this case, the output voltage of 14v filtered by the capacitor is then stabilized to a usable working voltage of 5v which is the required voltage utilized by the PIC 16F84 microcontroller and also 12v that is required by the relays RL1 and RL2.

The various stages in the design and implementation of the prototype system is shown in Figures 7, 8, and 9.



Figure 7. Remote Control (Transmitter Unit)

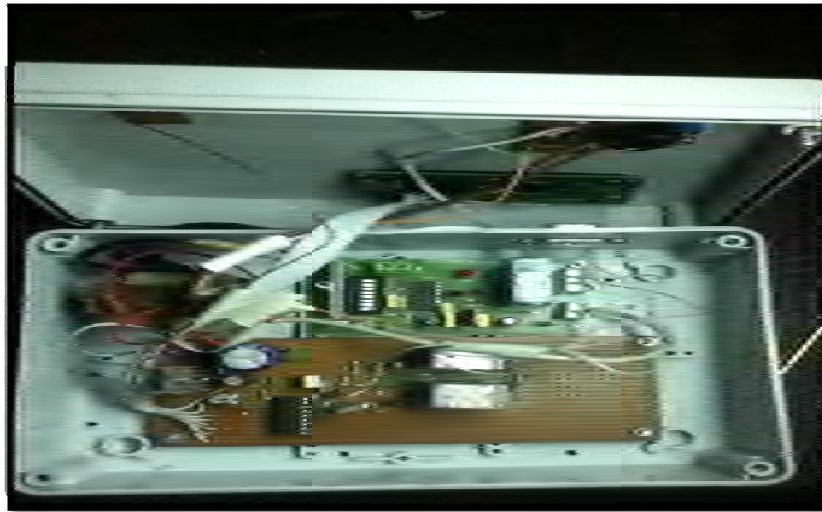


Figure 8. Remote Control (Receiver Unit)

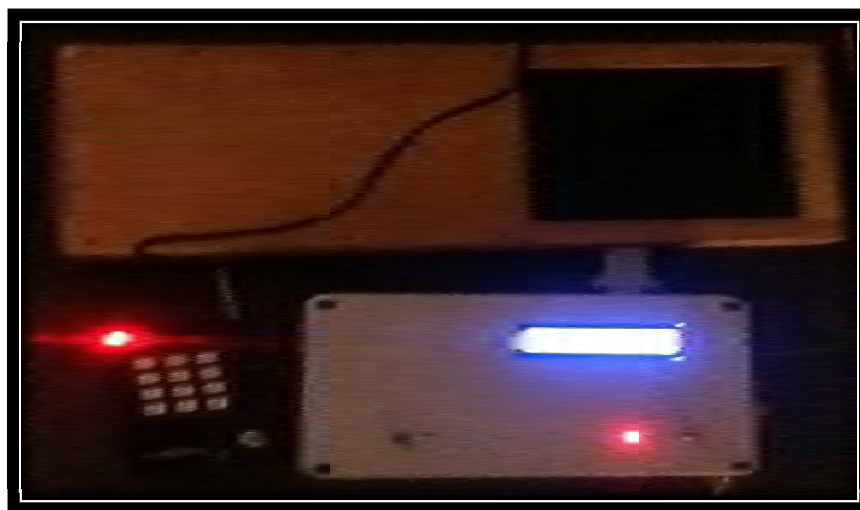


Figure 9. Remote Control (Complete Unit)

V. CONCLUSION

The construction of this project was as a result of the never ending demand for more effective security by individuals, companies and the society as a whole. This project is an answer to that demand and it has evolved from the norm of having a credential such as a key or an RFID tag to the use of a pass-code as the credential which makes it more peculiar to the individual with this information, hence optimizing security. At the end of the design and construction of the system, we were able to achieve a complete working system made of two units; i.e. the transmitter and the receiver unit and also the sliding door mechanism. That is able to give to the bearer of the password access to whatever unit, object or device they chose to gain entry to. Without this code, the user is unable to gain entry, thereby restricting the user.

REFERENCES

- [1] Rankl, W., W. Effing . Smart Card Handbook. John Wiley & Sons, 1997.
- [2] "Surveillance & Identification: Identity", Caslon Analytics research, analysis and strategies consultancy, 2006.
- [3] Landt, Jerry, "Shrouds of Time: The history of RFID", 2001.